Guidelines for Securing Desktops and Laptops

This document contains recommended guidelines for Department of Education (Department) employees (i.e., teachers, administrators, staff members) to use in securing the Department's desktop and laptop computers. Recent trends in cyber security incidents show increasing data and identity theft which calls for a higher degree of vigilance and caution. An ounce of prevention by implementing these guidelines can prevent a time-consuming remediation and extensive repair costs.

These guidelines are primarily for DOE employees desktop/laptops. Computers used by students should NOT have any sensitive data stored on them and may be excluded from some of the guidelines such as the need to encrypt the files/hard disk or screen lock timeout.

Following are recommended guidelines:

1) Use strong passwords. Use a password that is at least 8 characters long. Use a mix of upper and lower case characters, with numbers and special characters such as a period ".", or dash "-", or underscore "_" in the password. Change your password periodically at least every six months.

2) Keep your password for your use only. Don't write your password on a sticky note and post it in close proximity to the desktop/laptop. Avoid prying eyes when typing in your password.

3) Activate screen lock on your desktop/laptop. When you are away from your computer for an extended period, the screen should lock and require a password to access it again.

4) Install anti-virus and anti-malware protection on your desktop/laptop and keep it up to date. An infected computer can get compromised, be remotely controlled by external users and have its data content stolen. The Department has a statewide license from McAfee for antivirus protection, which can be downloaded at http://oits.k12.hi.us/software from within the Department's network.

Because of license restrictions, it can only be used on Department desktop/laptops and is only accessible within our network.

5) Keep current with the desktop/laptop operating systems patches and system updates. Install critical security patches when they are made available by the vendor.

6) Encrypt the data files and hard disk if you need to store confidential data on your desktop/laptop. In the event the computer is stolen, it would make it more difficult for the thieves to extract the confidential data.

7) Avoid placing confidential data on flash drives, compact discs, or other storage devices that are easily taken, shared or accessed. Purge such devices containing confidential information when the information is no longer required or the transfer to a secure server is complete.

8) Keep periodic backups or disk images of all critical data that is stored on the desktop/laptop. Also, in the event that a desktop/laptop gets infected, it is often easier to re-image the computer from a clean backup rather than trying to clean out the virus /malware.

9) Avoid storing any confidential data on the desktop/laptop in the first place. If you access confidential data on the desktop/laptop, remove it as soon as it is not required.

10) Remember that the desktops/laptops are the property of the Department and are subject to possible audits. They are to be used for official Department business only and not for personal use.